APPGUARD

Case Study

Protect ATMs from Malware, NuSource Financial, LLC

Industry:

Banking/Financial Technology Services

Challenges:

- Protect ATMs from Malware Threat
- ATMs are Network Isolated & Low-Power
- End-Customers abhor Complexity

Outcome:

"Four Years Malware-Free! No Bloat, No Burden, No Disruptions. It's Simple to Roll-out & Easy to Forget!"

Allan Lenius, VP
NuSource Financial, LLC

About NuSource Financial

NuSource Financial is one of the fastest growing Bank Technology companies in the United States, supplying innovative ATM, Branch Transformation, and Security Solutions to over 700 Financial Institutions (FI). FI's do not want their ATMs dragging them into mastering all things IT and cybersecurity, relying on NuSource to keep the ATMs running optimally. NuSource's services achieves this in part by finding the best available tools in an ever-changing world of technology and risks. Success means customers get no distractions, no excuses.

Situation: Ineffective Anti-Malware Tools

Headlines abound of Jackpotting and other advanced malware compromising ATMs. Anti-malware defenses rely less on preventing compromises and more on reacting, which equates to distracting FI's. Worse, newer tools need near real-time Internet access for detection data.

ATMs must be network isolated and managed by 3rd parties. Tools needing Internet access complicate operations. Further, ATMs are low CPU, memory, and hard drive. Patching is timely but takes time. PCI compliance affects all. Likely anti-malware tools fall short of needs.

Solution: AppGuard

NuSource researched and evaluated well known anti-malware tools but selected AppGuard because it uniquely blocked malware attacks (prevention) yet presented none of the unfavorable characteristics of alternatives.

Machine learning antivirus was too new four years ago. But has since been shown to show marginal improvement over traditional antivirus. Endpoint Detection and Response, and Behavior Analytics, yield too many alerts investigations and result in incidents by design. Each FI's network provider must give such tools Internet access.

AppGuard is not a detection tool. It blocks attacks in real-time, does NOT need Internet access, and does NOT need analysts to investigate alerts and remediate incidents. Its endpoint zero-trust approach requires no Internet access. This meant it could be installed without constant central management, which renders such out of PCI scope. {Central management is available, however.} All indications pointed to simple preventative protection.

AppGuard's footprint was observed to be extremely small: 10 MB on hard drive, 10 MB memory, and 0.0% CPU (average), making it ideal for ATMs.

"Roll-out & Admin are Extremely Easy"

NuSource noted that previous Application Control tools had required considerable, costly, professional services to roll-out and maintain. "AppGuard blocks far more types of attacks than application control yet at a tiny fraction of the overhead and cost", said Lenius.

"We've had No Problems; it just Works!"

Advanced endpoint protection tools must not only block attacks but also must stay out of the way of lifecycle operations. "AppGuard has not complicated or hindered patching or configuration management. Our migrations from Windows XP to Windows 7 were not impacted by AppGuard. How could an advanced protection tool possibly be less disruptive to such migrations," said Lenius.

"No Malware Incidents"

NuSource supports about 700 FI's. With AppGuard protecting Windows-based ATMs made by Nautilus, Hyosung and NCR, none has experienced a malware compromise. No PCI compliance problems. And, no alerts triage, alerts investigations, or ATM remediations. AppGuard blocks known and unknown attacks (Tyupkin, Wannacry, JackPotting, etc.) in real-time, at the ATM.

"Phenomenal, We Install it on All ATMs"

Lenius concluded, "four years later, the AppGuard difference remains the same. It's the one solution that doesn't force trade-offs preventing more versus requiring constant tuning and attention. It's one of those solutions one hopes to find. It's perfect for us and our customers. They get the install and forget solution they seek. No complications, no disruptions, no malware problems, and no need for excuses. It just works!

"Our financial institution customers have what they want from AppGuard: Install & Forget"

Allan Lenius, VP
NuSource Financial, LLC

APPGUARD

(703) 786-8884
sales@appguard.us
www.appguard.us

New York, NY; Chantilly, VA; Raleigh-Durham, NC; San Diego, CA; Colorado Springs, CO; Baltimore, MD; Columbus, OH; Washington, DC USA; Tokyo, Japan; Prague, Czech Republic; London, UK; Milan, Italy; Istanbul, Turkey; San Paolo, Brazil

About AppGuard

People and organizations all over the world are ever more interconnected via the endpoint devices in their lives. AppGuard delivers simple, effective solutions to the complex security challenges that threaten the interests of organizations as well as those of their customers. These endpoints range from personal computers to smartphones/tablets to IoT devices. AppGuard solutions prevent endpoint compromise; facilitate high assurance device to device authentication on behalf of their users; attest to the security posture of both endpoints so one does not share sensitive data with a user with an untrustworthy endpoint; and protect the privacy of end-users through anonymized, high assurance device-to-device authentication so they can communicate securely without revealing personally identifiable information of the end-users.